CLAIMS

1. A copy protection system for a field programmable gate array comprising:

a factory-programmed logic device (CPLD) including an initial state generator, a first sequence generator and an encryption device; and

a field-programmable gate array device (FPGA) being programmed with a field-programmable gate array program and including a second sequence generator, a third sequence generator, a decryption device and a sequence comparison device, said second sequence generator being a replicate of said first sequence generator;

wherein said CPLD generates an initial state in said initial state generator, initializes said first sequence generator with said initial state, encrypts said initial state in said encryption device, and transmits said encrypted initial state to said FPGA;

said FPGA decrypts said encrypted initial state in said decryption device, initializes said second sequence generator with said initial state, generates a challenge sequence with said third sequence generator, transmits said challenge sequence to said first sequence generator and said second sequence generator; and

wherein said first sequence generator generates a first reply sequence based on said initial state and said challenge sequence and transmits said first reply sequence to said sequence comparison device, and said second sequence generator generates a second reply sequence based on said initial state and said challenge sequence and transmits said second reply sequence to said sequence comparison device, which compares said first and second reply sequences and enables operation of said FPGA program when said first and second reply sequences are identical.

2. The system of claim 1 wherein said initial state is encrypted a second time in said encryption device before transmission to said decryption device.

3. The system of claim 2 wherein said first encryption operation is carried out with a first key k_0, said second encryption is carried out with a second key k_1 and said decryption is carried out with a third key k_2 such that:

$$x_0=k_2^{-1}(k_1(k_0(x_0)));$$

wherein x_0 is said initial state.

4. The system of claim 3 wherein said second key k_1 operates as a license which enables authorized licensees of said FPGA program to use said FPGA program.

5. A copy protection system for a field programmable gate array comprising:

a factory-programmed logic device (CPLD) including an initial state generator, a first sequence generator and an encryption device; and

a field-programmable gate array device (FPGA) being programmed with a field-programmable gate array program and including a second sequence generator, a decryption device and a sequence comparison device, said second sequence generator being a replicate of said first sequence generator;

wherein said CPLD generates an initial state in said initial state generator, initializes said first sequence generator with said initial state, encrypts said initial state in said encryption device, and transmits said encrypted initial state to said FPGA;

said FPGA decrypts said encrypted initial state in said decryption device, and initializes said second sequence generator with said initial state; and

wherein said first sequence generator generates a first sequence based on said initial state and transmits said first sequence to said sequence comparison device, and said second sequence generator generates a second sequence based on said initial state and transmits said second reply sequence to said sequence comparison device, which compares said first and second sequences and enables operation of said FPGA program when said first and second sequences are identical.

6. The system of claim 5 wherein said FPGA further comprises a third sequence generator which generates a challenge sequence, transmits said challenge sequence to said first sequence generator and said second sequence generator; and

wherein said first sequence generator generates a first reply sequence based on said initial state and said challenge sequence and transmits said first reply sequence to said sequence comparison device, and said second sequence generator generates a second reply sequence based on said initial state and said challenge sequence and transmits said second reply sequence to said sequence comparison device, which compares said first and second reply sequences and enables operation of said FPGA program when said first and second reply sequences are identical.

7. The system of claim 6 wherein said initial state is encrypted a second time before transmission to said decryption device.

8. The system of claim 7 wherein said first encryption operation is carried out with a first key k_0, said second encryption is carried out with a second key k_1 and said decryption is carried out with a third key k_2 such that:

$$x_0=k_2^{-1}(k_1(k_0(x_0)));$$

wherein x_0 is said initial state.

9. The system of claim 8 wherein said second key k_1 operates as a license which enables authorized licensees of said FPGA program to use said FPGA program.

10. A method of copy protecting a field-programmable gate array comprising:

A. generating an initial state in a random bit generator of a programmable logic device;

B. inputting said initial state into a first sequence generator of said programmable logic device;

C. encrypting said initial state;

D. transmitting said encrypted initial state from said programmable logic device to said field-programmable gate array;

E. decrypting said initial state in said field-programmable gate array;

F. inputting said initial state into a second sequence generator of said field-programmable gate array;

G. generating a first sequence with said first sequence generator based on said initial state;

H. generating a second sequence in said second sequence generator based on said initial state;

I. comparing said first sequence to said second sequence; and

J. terminating operation of said field-programmable gate array if said first sequence is not identical to said second sequence.

11. The method of claim 10 further comprising:

K. generating a third sequence in a third sequence generator of said field-programmable gate array; and

L. inputting said third sequence into said first sequence generator and said second sequence generator;

wherein said first and second sequences are generated based on both said initial state and said third sequence.

12. The method of claim 10 wherein step C comprises encrypting said initial state with a first key k_0.

13. The method of claim 12 further comprising encrypting said initial state with a second key k_1 after step C.

14. The method of claim 13 wherein step E comprises decrypting said initial state with a third key k_2, such that:

$$x_0=k_2^{-1}(k_1(k_0(x_0)));$$

wherein x_0 is said initial state.

15. The system of claim 14 wherein said second key k_1 operates as a license which enables authorized licensees of said FPGA program to use said FPGA program.